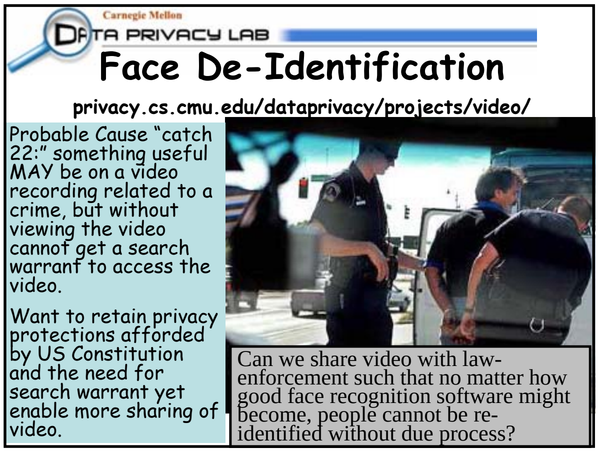
Face De-identification



Carnegie Mellon

DATA PRIVACY LAB

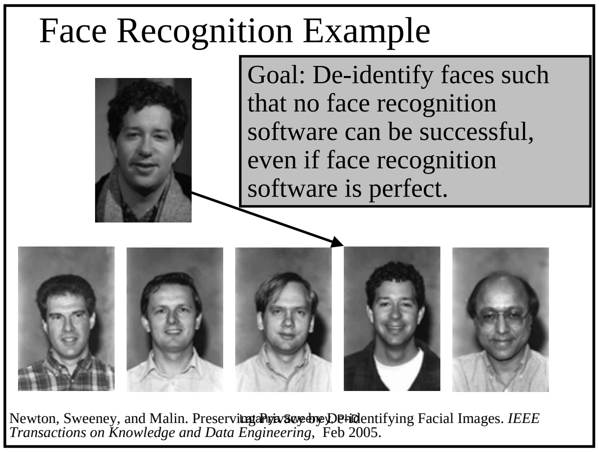
Face De-Identification

privacy.cs.cmu.edu/dataprivacy/projects/video/

Probable Cause "catch 22:" something useful MAY be on a video recording related to a crime, but without viewing the video cannot get a search warrant to access the video.

Want to retain privacy protections afforded by US Constitution and the need for search warrant yet enable more sharing of video.

Can we share video with law-enforcement such that no matter how good face recognition software might become, people cannot be re-identified without due process?

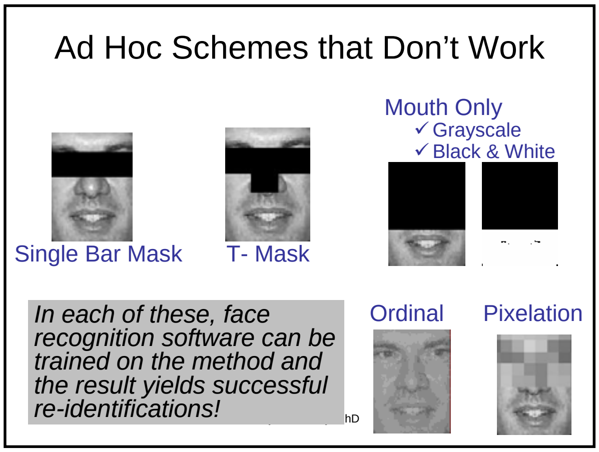


Face Recognition Example

Goal: De-identify faces such that no face recognition software can be successful, even if face recognition software is perfect.

Newton, Sweeney, and Malin. Preserving Privacy by De-identifying Facial Images. *IEEE Transactions on Knowledge and Data Engineering*, Feb 2005.

Latanya Sweeney, PhD



Ad Hoc Schemes that Don't Work

Single Bar Mask

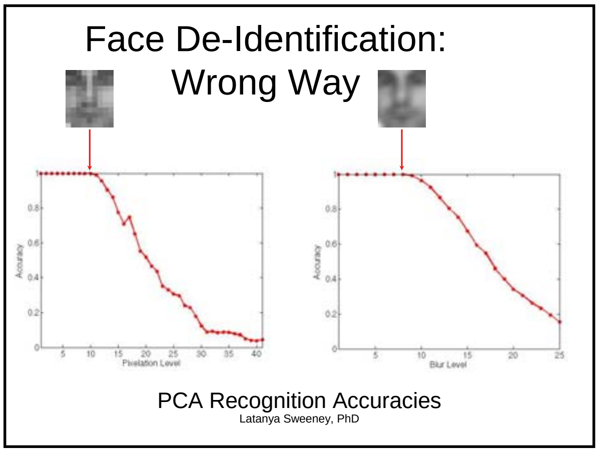
T- Mask

Mouth Only
✓ Grayscale
✓ Black & White

Ordinal

Pixelation

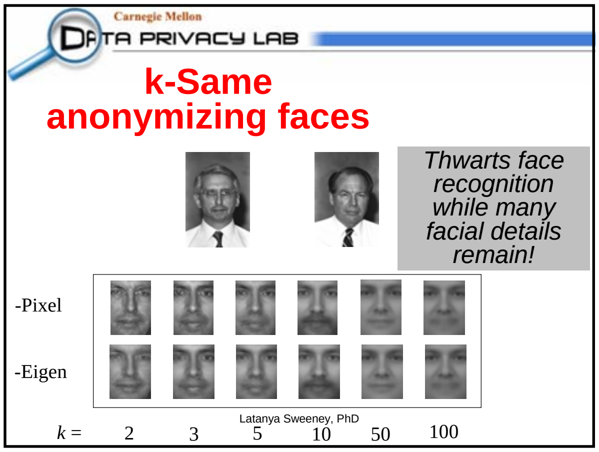
In each of these, face recognition software can be trained on the method and the result yields successful re-identifications!



Face De-Identification: Wrong Way

PCA Recognition Accuracies

Latanya Sweeney, PhD



Carnegie Mellon

DATA PRIVACY LAB

k-Same anonymizing faces

Thwarts face recognition while many facial details remain!

Latanya Sweeney, PhD

k-Same Works even as Face Recognition Software Improves

Theorem. There cannot exist any face recognition software for which a subject's k-Samed image can be correctly recognized better than 1/*k* probability.

Lessons learned

Ad hoc techniques don't work.

Useful images can be shared to detect suspicious activity, yet privacy protections are afforded.